(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : **0 528 730 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : **92402294.0**

(51) Int. Cl.^{5} : **G06F 12/14**

(22) Date de dépôt : **17.08.92**

(30) Priorité : **19.08.91 FR 9110404**

(43) Date de publication de la demande : **24.02.93 Bulletin 93/08**

(84) Etats contractants désignés : **BE DE GB SE**

(71) Demandeur : **FRANCE TELECOM**
Etablissement autonome de droit public, 6, Place d'Alleray
F-75015 Paris (FR)

(71) Demandeur : **TELEDIFFUSION DE FRANCE, société anonyme**
10 rue d'Oradour sur Glane
F-75015 Paris (FR)

(72) Inventeur : **Coutrot, Françoise**
Allée de la Croix Connue
F-35510 Cesson-Sevigne (FR)
Inventeur : **Fevrier, Pierre**
Rue des Trois Pignons
F-35250 St Sulpice la Foret (FR)

(74) Mandataire : **Mongrédien, André et al**
c/o BREVATOME 25, rue de Ponthieu
F-75008 Paris (FR)

(54) Procédés d'émission et de réception de programmes personnalisés.

(57) Procédés d'émission et de réception de programmes personnalisés.

Le programme est constitué d'éléments de programme personnalisés contenant une identification du destinataire, l'accès à chaque élément de programme étant réservé à son seul destinataire et conditionné à :

— la possession d'un titre d'accès qui couvre les critères d'accès au service,

— la possession d'une identification propre à chaque destinataire. Le message de contrôle des titres d'accès permet aux usagers du service de calculer, à partir du seul cryptogramme d'un mot de contrôle racine et de l'identification du destinataire, tous les mots de contrôle personnalisés qui permettront à chaque destinataire (et à lui seul) de désembrouiller les éléments qui le concernent.

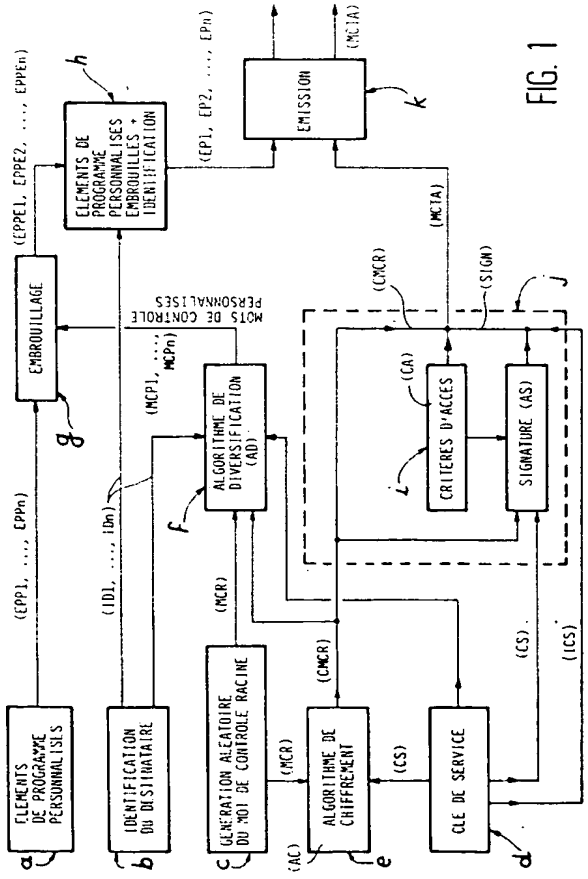

FIG. 1

EP 0 528 730 A1

La présente invention a pour objet un procédé d'émission et un procédé de réception de programmes personnalisés.

La forte augmentation des supports de diffusion (satellites, câbles, herztien) amène les opérateurs de programmes à multiplier les offres de services pour des programmes à contrôle d'accès, qu'il s'agisse de programmes audiovisuels, sonores ou de transmission de données.

Le principe du contrôle de l'accès à de tels services repose sur l'embrouillage d'un programme à l'émission et sur le désembrouillage du message reçu sous le contrôle d'un titre d'accès. Les systèmes d'embrouillage et de désembrouillage sont initialisés par une donnée qui varie aléatoirement, appelée mot de contrôle. Les informations décrivant les critères d'accès au programme ainsi qu'une forme protégée du mot de contrôle sont incluses dans des messages de contrôle des titres d'accès, messages qui accompagnent le programme embrouillé.

Pour accéder à un programme embrouillé, il faut que le dispositif d'accès conditionnel puisse exploiter un des messages de contrôle des titres d'accès associés au programme. Dans le cas de services "personnalisés", pour lesquels le programme est composé d'une multitude d'éléments de programme (séquences vidéo et/ou sons et/ou données) adressés à autant de destinataires différents, chaque élément de programme ne doit être restitué en clair qu'à son seul destinataire et les messages de contrôle des titres d'accès doivent permettre de garantir la protection de chacun des éléments de programme.

La présente invention a pour objet un procédé d'émission et de réception de messages de contrôle des titres d'accès qui permette à tout destinataire (mais à lui seul) de recevoir les éléments de programme qui lui sont adressés dans le cadre d'un service de diffusion personnalisé.

Les applications d'un tel procédé sont tous les services de diffusion de programmes personnalisés multiplexés sur un même support de diffusion. Ainsi, par exemple, la messagerie vocale, la diffusion de données (télex, téléchargement de données, télécopie diffusée, radiomessagerie (Opérator, Alphapage, ...), la diffusion d'images fixes ou animées (vidéotransmission, ...).

Etat de la technique antérieure

Les procédés actuels permettant de protéger l'accès à un programme diffusé consistent à affecter à chaque élément de programme un message de contrôle des titres d'accès. Cette technique est largement utilisée dans les services de télévision à péage pour lesquels chaque programme ou élément de programme concerne une audience importante et donc pour lesquels il suffit d'associer un ou plusieurs (typiquement 3 voire 4) messages de contrôle des titres d'accès à l'ensemble du programme diffusé. Le débit des informations spécifiques au contrôle d'accès relativement à un programme diffusé est alors très faible (typiquement quelques centaines d'octets par seconde pour contrôler un débit d'informations de plusieurs Mégaoctets par seconde).

Chaque message de contrôle des titres d'accès comporte en général quatre champs :

- un identificateur de la clé de service à utiliser,
- un champ précisant les conditions d'accès à satisfaire pour avoir le droit d'utiliser cette clé de service,
- le(s) cryptogramme(s) d'un ou de deux mots de contrôle,
- un champ de redondance, qui peut être utilement ajouté afin que le processeur de sécurité ne puisse être utilisé en dehors du contexte prévu.

Quand le processeur de sécurité contient un droit d'accès convenable, c'est-à-dire quand il détient la clé de service indiquée par l'identificateur et que cette clé est munie d'un statut compatible avec certaines des conditions indiquées dans le champ de critères d'accès, le processeur de sécurité déchiffre le(s) cryptogramme(s) pour reconstituer le(s) mot(s) de contrôle.

Le mot de contrôle permet au terminal de désembrouiller le programme ou les éléments de programme auxquels il est associé.

Dans le cas de services de diffusion personnalisés, l'extension de la technique précédente, qui consisterait à associer autant de messages de contrôle des titres d'accès qu'il y a d'éléments de programme accessibles de façon distincte, amènerait à diminuer, dans certains cas, la ressource d'informations par deux, en considérant que le contenu de l'information à transmettre est du même ordre d'encombrement que le message de contrôle des titres d'accès lui-même (cas de radiomessageries affichant 40 caractères).

Cette forte diminution de la ressource utile restante (l'information elle-même) va à l'encontre de la rentabilité économique recherchée pour le service diffusé.

Exposé de l'invention

La présente invention a justement pour but de remédier à cet inconvénient. A cette fin, la présente invention prévoit un procédé dans lequel le programme est décomposé en autant d'éléments de programme qu'il y a de séquences personnalisées (vidéo et/ou sons et/ou données), ces éléments étant repérés par une identification propre à leur destinataire et ayant un contenu embrouillé à partir d'un mot de contrôle qui est spécifique à chaque destinataire, ce qui garantit la confidentialité des séquences de programme.

Au programme diffusé est associé un message

de contrôle des titres d'accès qui va permettre à l'ensemble des processeurs de sécurité des usagers autorisés de reconstituer, à partir du cryptogramme d'un mot de cont ôle général appelé mot de contrôle "racine" et de l'identification de chaque destinataire, le mot de contrôle spécifique qui permettra le désembrouillage des éléments de programme repérés par cette même identification du destinataire.

L'invention permet, tout en garantissant une confidentialité totale de chacun des éléments de progr mme, de ne diffuser qu'un seul message de contrôle des titres d'accès à partir duquel tous les destinataires de séquences de programme pourront calculer le mot de contrôle personnalisé ayant servi à embrouiller en amont les informations qui les concernent.

Un tel procédé permet de revenir à des débits d'informations identiques à ceux des services de télévision à péage, à savoir quelques centaines d'octets par seconde.

De façon précise, l'invention a pour objet un procédé d'émission de programmes personnalisés, dans lequel on embrouille les programmes par un mot de contrôle et on forme des messages de contrôle d'accès contenant, notamment, des critères d'accès et un cryptogramme du mot de contrôle, ce procédé étant caractérisé par le fait que, pour adresser des programmes personnalisés à divers destinataires repérés par des identificateurs, le mot de contrôle utilisé pour embrouiller le programme destiné à un destinataire particulier est obtenu par personnalisation, à l'aide de l'identificateur de ce destinataire, d'un mot de contrôle unique dit mot de contrôle "racine", valable pour tous les destinataires et on n'émet qu'un seul message de contrôle d'accès pour tous les destinataires, ce message contenant, notamment, un cryptogramme du mot de contrôle racine.

La présente invention a également pour objet un procédé de réception de programmes émis selon le procédé d'émission précédent. Ce procédé est du genre de ceux dans lesquels on vérifie si les critères d'accès sont remplis, on reconstitue le mot de contrôle ayant servi à l'embrouillage et on désembrouille les programmes reçus, et il est caractérisé par le fait que chaque destinataire, à l'aide de son identificateur et du message de contrôle d'accès, reconstitue, à partir du mot de contrôle racine, le mot de contrôle personnalisé qui lui est propre, ce qui lui permet et à lui seul, de désembrouiller le programme qui lui est destiné.

L'invention peut être mise en oeuvre soit à l'émission, soit à la réception, soit à la fois à l'émission et à la réception.

Brève description des dessins

- la figure 1 montre de manière générale les diverses opérations effectuées à l'émission,
- la figure 2 illustre la structure générale d'un programme diffusé,
- la figure 3 illustre la structure d'un message de contrôle des titres d'accès,
- la figure 4 montre de manière générale les diverses opérations effectuées à la réception par un dispositif d'accès,
- la figure 5 montre la structure particulière d'un message de contrôle des titres d'accès,
- la figure 6 illustre le format d'un message de type "protocole Général Purpose Data" (GPD),
- la figure 7 illustre la structure d'un en-tête de message,
- la figure 8 illustre l'extension d'un en-tête de message,
- la figure 9 illustre un champ d'adresse étendue,
- la figure 10 montre une première variante des moyens permettant d'obtenir, à l'émission, un mot de contrôle personnalisé,
- la figure 11 montre une seconde variante des moyens permettant d'obtenir un mot de contrôle personnalisé,
- la figure 12 montre une première variante des moyens permettant, à la réception, de restituer un mot de contrôle personnalisé lorsque la première variante a été utilisée à l'émission pour obtenir ledit mot de contrôle personnalisé,
- la figure 13 montre une seconde variante des moyens permettant, à la réception, de restituer un mot de contrôle personnalisé lorsque la seconde variante a été utilisée à l'émission pour obtenir ledit mot de contrôle personnalisé.

Exposé détaillé des modes de réalisation

Sur la figure 1 (ainsi que sur d'autres figures générales comme les figures 4, 10, 11, 12, 13, ...), les différents blocs représentés correspondent à diverses opérations. On ne doit pas considérer que ces opérations sont effectuées par autant de circuits indépendants. L'homme du métier sait que ces opérations sont le plus souvent effectuées globalement, par des microprocesseurs, tant à l'émission qu'à la réception.

La figure 1 illustre les opérations essentielles effectuées à l'émission.

Les références littérales (a, b, c, ...) employées sur cette figure correspondent aux paragraphes suivants :

a) on divise le programme à émettre en (n) éléments de programme dits "éléments de programme personnalisés" (EPP1, EPP2, ..., EPPn) destinés à (n) destinataires différents (D1, D2, ..., Dn) ;

b) on affecte à chaque destinataire (D1, D2, ..., Dn) un identificateur (ID1, ID2, ..., IDn) ;

c) on engendre de manière aléatoire un mot de contrôle, valable pour tous les destinataires, appelé "mot de contrôle racine" (MCR) ;

d) on définit une clé de service (CS) par un identificateur de clé de service (ICS) ;

e) à partir du mot de contrôle racine (MCR) et de la clé de service (CS), on met en oeuvre un algorithme, dit de chiffrement (AC), pour obtenir un cryptogramme du mot de contrôle racine (CMCR) ;

f) à partir du mot de contrôle racine (MCR), de l'identification des destinataires (ID1, ID2, ..., IDn) et de la clé de service (CS), on met en oeuvre un algorithme, dit de diversification (AD), qui délivre des mots de contrôle propres à chaque destinataire (D1, D2, ..., Dn) dits "mots de contrôle personnalisés" (MCP1, MCP2, ..., MCPn) ;

g) à partir des éléments de programme personnalisés (EPP1, EPP2, ..., EPPn) et des mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) correspondant aux différents destinataires (D1, D2, ..., Dn) visés, on embrouille lesdits éléments de programme personnalisés (EPP1, EPP2, ..., EPPn) à l'aide respectivement desdits mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) pour obtenir des éléments de programme personnalisés embrouillés (EPPE1, EPPE2, ..., EPPEn) ;

h) on adjoint à ces éléments de programme personnalisés embrouillés les identificateurs des destinataires (ID1, ID2, ..., IDn) pour constituer des éléments de programme (EP1, EP2, ..., EPn) propres à ces différents destinataires ;

i) on définit des critères d'accès (CA) auxquels il faut satisfaire pour avoir le droit d'utiliser la clé de service (CS) ;

j) à partir de l'identificateur de clé de service (ICS), du cryptogramme du mot de contrôle racine (CMCR), des critères d'accès (CA) et éventuellement d'une signature de ce cryptogramme et des critères d'accès (SIGN), on forme des messages de contrôle des titres d'accès (MCTA) ;

k) on émet les éléments de programme embrouillés (EP1, EP2, ..., EPn) ainsi que les messages de contrôle des titres d'accès (MCTA).

La figure 2 montre la structure générale des éléments de programme (EP1), ... (EPn) avec leurs identificateurs de destinataires, respectivement (ID1), ... (IDn) associés aux éléments de programme personnalisés embrouillés, respectivement (EPPE1), ... (EPPEn). Peut s'ajouter à ces (n) blocs, un bloc de données de service (DS), non personnalisées (service de diffusion à large audience) ou des données de service permettant de décrire la structure propre au service.

Le message de contrôle des titres d'accès (MCTA), qui inclut les critères d'accès au programme et les informations contenant le cryptogramme du mot de contrôle racine (CMCR), peut avoir une structure telle que celle de la figure 3 où l'on voit un identificateur de clé de service (ICS) suivi des critères d'accès au service (CA), suivis du cryptogramme du mot de contrôle racine (CMCR), avec, enfin (et éventuellement) la signature (SIGN) des critères d'accès et du cryptogramme du mot de contrôle racine.

La suite des opérations effectuées dans le terminal de l'un des destinataires, par exemple le destinataire de rang i (i étant un entier compris entre 1 et n), est représenté schématiquement sur la figure 4. Ces opérations sont définies dans les paragraphes suivants où le numéro du paragraphe se réfère encore à la référence littérale servant à repérer les blocs sur la figure :

l) chaque destinataire reçoit les éléments de programme embrouillés (EP1, EP2, ..., EPn) avec leurs identificateurs de destinataires (ID1, ID2, ..., IDn) et leurs éléments de programme personnalisés embrouillés (EPPE1, EPPE2, ..., EPPEn) et reçoit aussi les messages de contrôle des titres d'accès (MCTA) ;

m) le destinataire particulier (Di) retient, parmi les éléments de programme qu'il reçoit, ceux qui contiennent son identificateur (IDi), ce qui lui donne les éléments de programmes personnalisés embrouillés (EPPEi) qui lui sont destinés ;

n) ce destinataire particulier (Di), à partir des messages de contrôle des titres d'accès (MCTA), vérifie si les critères d'accès (CA) sont remplis par le titre d'accès qu'il possède ; le cas échéant, il vérifie l'intégrité du message par analyse de la signature (SIGN) si celle-ci a été effectuée à l'émission ;

o) à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS), et de son identificateur IDi), le destinataire (Di) met en oeuvre un algorithme inverse (AC^{-1}) de l'algorithme de chiffrement (AC) qui a été mis en oeuvre à l'émission dans l'opération e) ; il met également en oeuvre un algorithme (AD) qui est l'algorithme de diversification (AD) qui a été mis en oeuvre à l'émission dans l'opération f) ; il retrouve finalement le mot de contrôle personnalisé qui lui est propre (MCPi) ;

p) le destinataire (Di) désembrouille alors les éléments de programme personnalisés embrouillés (EPPEi) qui qui sont destinés, obtenus après l'opération m) à partir du mot de contrôle personnalisé (MCPi) obtenu après l'opération o) et obtient, en clair, les éléments de programme personnalisé (EPPi) qui lui sont propres.

Un mode de réalisation va être décrit maintenant, qui s'applique aux signaux de la famille MAC/Paquet-EUROCRYPT (y compris dans le mode de diffusion de données plein canal).

La structure des messages de contrôle des titres d'accès est telle que définie dans la spécification du système d'accès conditionnel EUROCRYPT applicable aux signaux de la famille MAC/Paquet. Elle est il-

lustrée sur la figure 5 : l'identificateur de clé de service (ICS) désigne une clé secrète (CS) et s'étend sur 3 octets ; les critères d'accès (CA) sur un nombre d'octets variable ; le ou les cryptogramme(s) du mot de contrôle racine (CMCR) obtenu à l'aide de la clé secrète (CS) s'étend(ent) sur 8 ou 16 octets ; enfin, la signature s'étend sur 8 octets.

Cette signature est le résultat d'un algorithme de compression appliqué aux informations présentes dans le message de contrôle des titres d'accès (critères d'accès et cryptogramme(s) du mot de contrôle) en utilisant la clé secrète (CS).

Les formats des messages correspondant à la diffusion de données numériques (télétexte, sons, ...) sont décrits dans la partie 4C du document de spécification d'un signal MAC/Paquet sous le vocable "Protocole General Purpose Data (GPD)". La structure de ces messages est illustrée sur la figure 6 où le message comprend, en tout, 45 octets avec un en-tête de message variable, un segment de données variable et un champ de code de détection d'erreur "Code à Redondance Cyclique" (CRC) optionnel.

L'en-tête de message est illustré sur la figure 7 avec un descripteur de format sur 1 octet et une extension de l'en-tête de message de longueur variable. Le descripteur précise si le champ d'extension d'entête de message est présent, si le compteur de segment est présent et si le champ d'adresse est présent.

La figure 8 illustre l'extension de l'en-tête de message avec un champ d'adresse étendue variable, un compteur de segment (optionnel) sur 4 octets et une longueur de segment (optionnel) sur 3 octets.

Enfin, la figure 9 illustre le champ d'adresse étendue avec une longueur d'adresse sur un octet et une adresse étendue de longueur variable.

Il est proposé d'identifier les messages au format GPD en précisant dans le champ "adresse étendue", l'adresse unique (UA) (5 octets) telle que décrite dans la spécification EUROCRYPT. Cette adresse caractérise de façon unique chacun des processeurs de sécurité des usagers.

A noter que le procédé d'identification des messages peut également être intégré au niveau "applicatif" du message, donc dépendant de la nature des informations échangées à l'intérieur des segments de données.

Les figures 10 et 11 montrent deux variantes, parmi les réalisations possibles, d'obtention d'un mot de contrôle personnalisé à partir, soit du mot de contrôle racine soit du cryptogramme du mot de contrôle racine. Ces deux variantes sont utilisées l'émission. Il leur correspond deux variantes utilisées à la réception et qui seront décrites en liaison avec les figures 12 et 13.

Dans la variante illustrée sur la figure 10, pour obtenir, dans l'opération f) définie plus haut, des mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) à partir du mot de contrôle racine (MCR), de l'identification des destinataires défini par une adresse unique (UA) et de la clé de service (CS), on applique l'algorithme de diversification (AD) au mot de contrôle racine avec l'adresse unique (UA) du destinataire comme paramètre de diversification. Pour obtenir le cryptogramme du mot de contrôle racine, on applique l'algorithme de chiffrement (AC) au mot de contrôle racine (MCR) en prenant la clé de service (CS) comme paramètre de chiffrement.

Dans la variante de la figure 11, on applique l'algorithme de diversification (AD) à la clé de service (CS) en prenant l'adresse unique comme paramètre de diversification, ce qui donne une clé de service personnalisée (CSP) ; puis on applique l'algorithme de déchiffrement (AC^{-1}) au cryptogramme du mot de contrôle racine (CMCR) en prenant la clé de service personnalisée (CSP) comme paramètre de chiffrement.

A la réception, dans le cas de la première variante illustrée sur la figure 12, pour obtenir, à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS) et de l'adresse (UA), le mot de contrôle personnalisé (MCPi) qui est propre au destinataire (Di), on commence par appliquer au cryptogramme du mot de contrôle racine (CMCR) l'algorithme de déchiffrement inverse (AC^{-1}) en pre ant la clé de service (CS) comme paramètre de déchiffrement, ce qui donne le mot de contrôle racine (MCR) ; puis on applique à ce mot de contrôle racine (MCR) l'algorithme de diversification inverse (AD) en prenant l'adresse unique (UA) comme paramètre de diversification, ce qui donne finalement le mot de contrôle personnalisé (MCPi) qui lui est propre.

Dans la seconde variante, illustrée sur la figure 13, pour obtenir, à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS) et de l'adresse unique (UA), le mot de contrôle personnalisé qui est propre au destinataire (Di), on commence par appliquer l'algorithme de diversification (AD) à la clé de service (CS), avec l'adresse (UA) comme paramètre de diversification, ce qui donne la clé de service personnalisée (CSP) ; puis on applique l'algorithme de déchiffrement (AC^{-1}) au cryptogramme du mot de contrôle racine (CMCR) en prenant la clé de service personnalisée (CSP) comme paramètre de déchiffrement, ce qui donne finalement le mot de contrôle personnalisé (MCPi) qui est propre au destinataire (Di).

Dans quelle que variante que ce soit, ayant obtenu le mot de contrôle personnalisé, on applique à un générateur pseudo-aléatoire délivrant des suites déchiffrantes qui correspondent aux suites chiffrantes utilisées à l'émission.

Les moyens pour embrouiller et désembrouiller les segments de données peuvent être constitués classiquement par des portes OU-exclusif, dont une entrée reçoit les suites chiffrantes/déchiffrantes et l'autr les données en clair/embrouillées et dont la sortie délivre les données embrouillées/en clair.

Dans la réalisation pratique, le traitement effectué par le dispositif d'accès conditionnel en émission/réception est intégralement réalisé par un processeur de sécurité (carte à mémoire) pour un débit in érieur ou égal à 2400 bauds (avec les technologies de cartes à mémoire actuelles). Le processeur délivre les suites chiffrantes/déchiffrantes à appliquer aux données à embrouiller/désembrouiller. En cas de débit supérieur, la fonction de génération pseudo-aléatoire est déportée dans le terminal et le processeur délivre les mots de contrôle personnalisés.

Revendications

1. Procédé d'émission de programmes personnalisés, dans lequel on embrouille les programmes par un mot de contrôle et on forme des messages de contrôle d'accès contenant, notamment, des critères d'accès et un cryptogramme du mot de contrôle, ce procédé étant caractérisé par le fait que, pour adresser des programmes personnalisés à divers destinataires repérés par des identificateurs, le mot de contrôle utilisé pour embrouiller le programme destiné à un destinataire particulier est obtenu par personnalisation, à l'aide de l'identificateur de ce destinataire, d'un mot de contrôle unique dit mot de contrôle "racine", valable pour tous les destinataires et on n'émet qu'un seul message de contrôle d'accès pour tous les destinataires, ce message contenant, notamment, un cryptogramme du mot de contrôle racine.

2. Procédé selon la revendication 1, caractérisé par le fait qu'il comprend les opérations suivantes :
   a) on divise le programme à émettre en divers (n) éléments de programme dits éléments de programme personnalisés (EPP1, EPP2, ..., EPPn) destinés à autant (n) de destinataires différents (D1, D2, ..., Dn) ;
   b) on affecte à chaque destinataire (D1, D2, ..., Dn) un identificateur (ID_1, ID_2, ..., ID_n) ;
   c) on engendre de manière aléatoire un mot de contrôle valable pour tous les destinataires, appelé mot de contrôle racine (MCR) ;
   d) on définit une clé de service (CS) par un identificateur de clé de service (ICS) ;
   e) à partir du mot de contrôle racine (MCR) et de la clé de service (CS), on met en oeuvre un algorithme de chiffrement (AC) pour obtenir un cryptogramme du mot de contrôle racine (CMCR) ;
   f) à partir du mot de contrôle racine (MCR) ou du cryptogramme du mot de contrôle racine (CMCR), de l'identification des destinataires (ID_1, ID_2, ..., ID_n) et de la clé de service (CS), on met en oeuvre un algorithme de diversification (AD) qui délivre des mots de contrôle propres à chaque destinataires (D1, D2, ..., Dn), dits mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) ;
   g) à partir des éléments de programme personnalisés (EPP1, EPP2, ..., EPPn) et des mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) correspondant aux différents destinataires (D1, D2, ..., Dn) visés, on embrouille lesdits éléments de programme personnalisés (EPP1, EPP2, ..., EPPn) à l'aide respectivement desdits mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) pour obtenir des éléments de programme personnalisés embrouillés (EPP1, EPP2, ..., EPPn) ;
   h) on adjoint à ces éléments de programme personnalisés embrouillés les identificateurs des destinataires (ID1, ID2, ..., IDn) pour constituer des éléments de programme (EP1, EP2, ..., EPn) propres à ces différents destinataires ;
   i) on définit des critères d'accès (CA) auxquels il faut satisfaire pour avoir le droit d'utiliser la clé de service (CS) ;
   j) à partir du cryptogramme du mot de contrôle racine (CMCR), de l'identificateur de clé de service (ICS), des critères d'accès (CA) et éventuellement d'une signature (SIGN) de ce cryptogramme et des critères d'accès, on forme des messages de contrôle des titres d'accès (MCTA) ;
   k) on émet les éléments de programme (EP1, EP2, ..., EPn) ainsi que les messages de contrôle des titres d'accès (MCTA).

3. Procédé selon la revendication 2, caractérisé par le fait que pour obtenir, dans l'opération f), des mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) à partir du mot de contrôle racine (MCR), de l'identification des destinataires (ID1, ID2, ..., IDn) et de la clé de service (CS), on applique l'algorithme de diversification (AD) au mot de contrôle racine avec la clé de service (CS) et l'adresse unique (UA) du destinataire comme paramètre de diversification (Fig. 10).

4. Procédé selon la revendication 2, caractérisé par le fait que pour obtenir, dans l'opération f), des mots de contrôle personnalisés (MCP1, MCP2, ..., MCPn) à partir du mot de contrôle racine (MCR), de l'identification des destinataires (ID1, ID2, ..., IDn) et de la clé de service (CS), on applique l'algorithme de diversification (AD) à la clé de service (CS) en prenant l'adresse unique comme paramètre de diversification ce qui donne une clé de service personnalisée (CSP) puis, on applique l'algorithme de déchiffrement (AC^{-1}) au

cryptogramme du mot de contrôle racine (CMCR) en prenant la clé de service personnalisée (CSP) comme paramètre de déchiffrement (Fig. 11).

5. Procédé de réception de programmes émis par le procédé selon l'une quelconque des revendications 1 à 4, dans lequel on vérifie si les critères d'accès sont remplis, on reconstitue le mot de contrôle ayant servi à l'embrouillage et on désembrouille les programmes reçus, caractérisé par le fait que chaque destinataire, à l'aide de son identificateur et du message de contrôle d'accès, reconstitue, à partir du mot de contrôle racine, le mot de contrôle personnalisé qui lui est propre, ce qui lui permet et à lui seul, de désembrouiller le programme qui lui est destiné.

6. Procédé de réception selon la revendication 5, pour des programmes émis selon la revendication 2, caractérisé par le fait que :

l) chaque destinataire reçoit les éléments de programme (EP1, EP2, ..., EPn) avec leurs identificateurs de destinataires (ID1, ID2, ..., IDn) et leurs éléments de programme personnalisés embrouillés (EPPE1, EPPE2, ..., EPPn) et reçoit aussi les messages de contrôle des titres d'accès (MCTA) ;

m) un destinataire particulier (Di) retient, dans les éléments de programme reçus, ceux qui contiennent l'identificateur qui lui correspond (IDi), ce qui lui donne les éléments de programmes personnalisés embrouillés (EPPEi) qui lui sont destinés ;

n) le destinataire (Di), à partir des messages de contrôle des titres d'accès (MCTA) vérifie si les critères d'accès (CA) sont remplis par le titre d'accès qu'il possède ; le cas échéant, il vérifie l'intégrité du message par analyse de la signature si celle-ci a été effectuée à l'émission ;

o) à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS), et de son identificateur (IDi), le destinataire (Di) met en oeuvre l'algorithme inverse (AC^{-1}) de l'algorithme de chiffrement (AC) mis en oeuvre à l'émission dans l'opération e) et met en oeuvre l'algorithme (AD) de diversification (AD) mis en oeuvre à l'émission dans l'opération f) pour retrouver le mot de contrôle personnalisé qui lui est propre (MCPi) ;

p) le destinataire (Di) désembrouille alors les éléments de programme personnalisés embrouillés (EPPEi) qui lui sont destinés obtenus après l'opération m) à partir du mot de contrôle personnalisé (MCPi) obtenu après l'opération o) et obtient en clair les éléments de programme personnalisé (EPPi) qui lui sont propres.

7. Procédé de réception selon la revendication 6, pour des programmes émis selon la revendication 3, caractérisé par le fait que pour obtenir, dans l'opération o), à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS) et de l'identificateur (IDi), le mot de contrôle personnalisé qui lui est propre (MCPi), le destinataire (Di) commence par appliquer au cryptogramme du mot de contrôle racine (CMCR) l'algorithme de déchiffrement (AC^{-1}) inverse de l'algorithme de chiffrement (AC) en prenant la clé de service (CS) comme paramètre, ce qui lui donne le mot de contrôle racine (MCR), puis il applique à ce mot de contrôle racine (MCR) l'algorithme de diversification (AD) en prenant l'adresse unique (UA) comme paramètre de diversification, ce qui lui donne finalement le mot de contrôle personnalisé (MCPi) qui lui est propre (Fig. 12).

8. Procédé de réception selon la revendication 7, de programmes émis selon la revendication 4, caractérisé par le fait que pour obtenir, dans l'opération o), à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS) et de l'identificateur (IDi), le mot de contrôle personnalisé qui lui est propre (MCPi), le destinataire (Di) commence par appliquer l'algorithme de diversification (AD) à la clé de service (CS) avec l'adresse (UA) comme paramètre de diversification, ce qui lui donne la clé de service personnalisée (CSP), puis il applique l'algorithme de déchiffrement (AC^{-1}) au cryptogramme du mot de contrôle racine (CMCR) en prenant la clé de service personnalisée (CSP) comme paramètre de déchiffrement, ce qui lui donne finalement le mot de contrôle personnalisé (MCPi) qui lui est propre (Fig. 13).

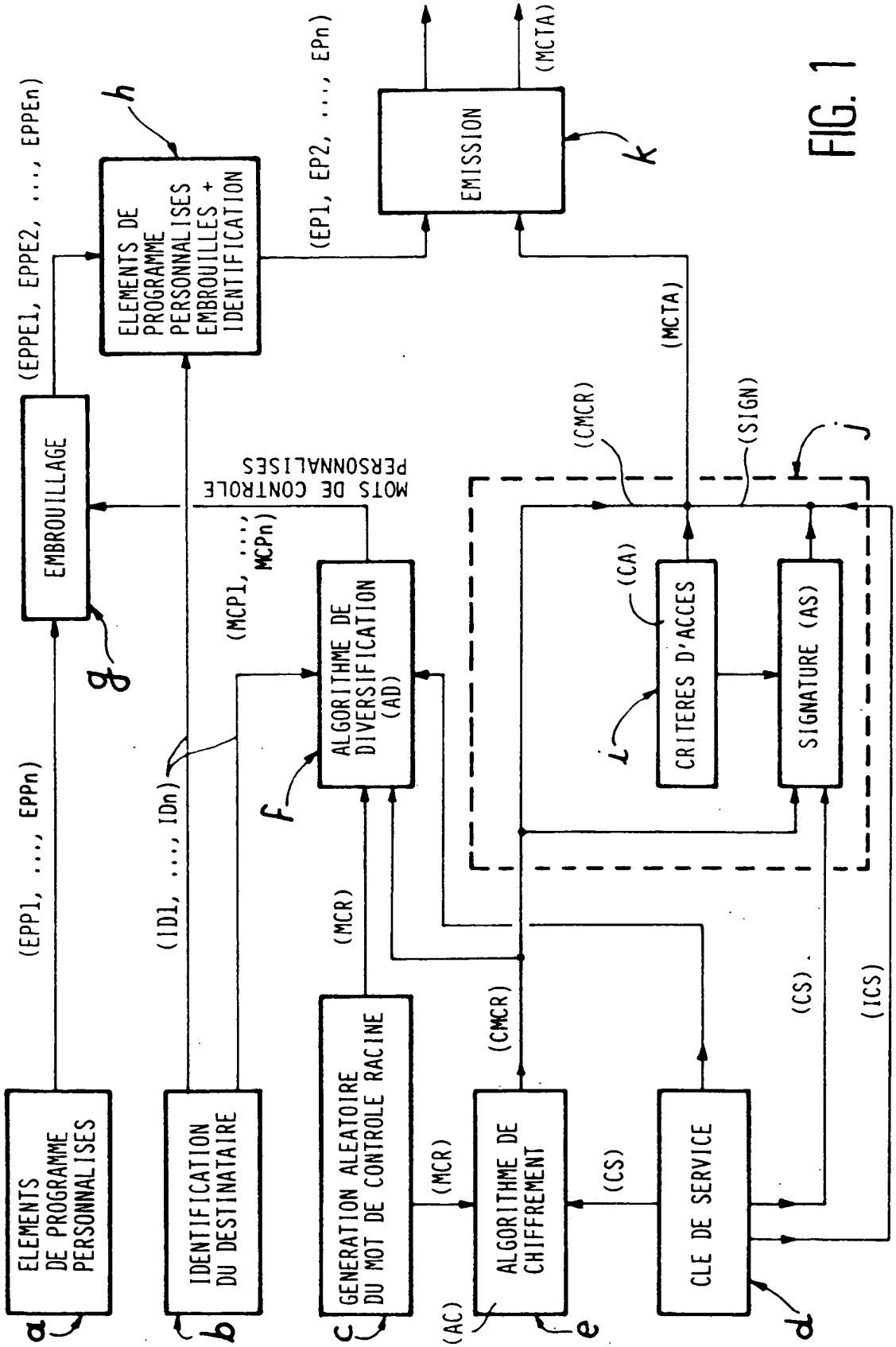
ELEMENTS DE PROGRAMME PERSONNALISES
a
(EPP1, ..., EPPn)
IDENTIFICATION DU DESTINATAIRE
b
(ID1, ..., IDn)
GENERATION ALEATOIRE DU MOT DE CONTROLE RACINE
c
(MCR)
ALGORITHME DE CHIFFREMENT
e
(AC)
(CS)
CLE DE SERVICE
d
(CS)
(ICS)
(CMCR)
ALGORITHME DE DIVERSIFICATION (AD)
f
(MCP1, ..., MCPn)
MOTS DE CONTROLE PERSONNALISES
EMBROUILLAGE
g
(EPPE1, EPPE2, ..., EPPEn)
ELEMENTS DE PROGRAMME PERSONNALISES EMBROUILLES + IDENTIFICATION
h
(EP1, EP2, ..., EPn)
EMISSION
k
(MCTA)
(MCTA)
(CMCR)
(SIGN)
j
(CA)
CRITERES D'ACCES
i
SIGNATURE (AS)

FIG. 1

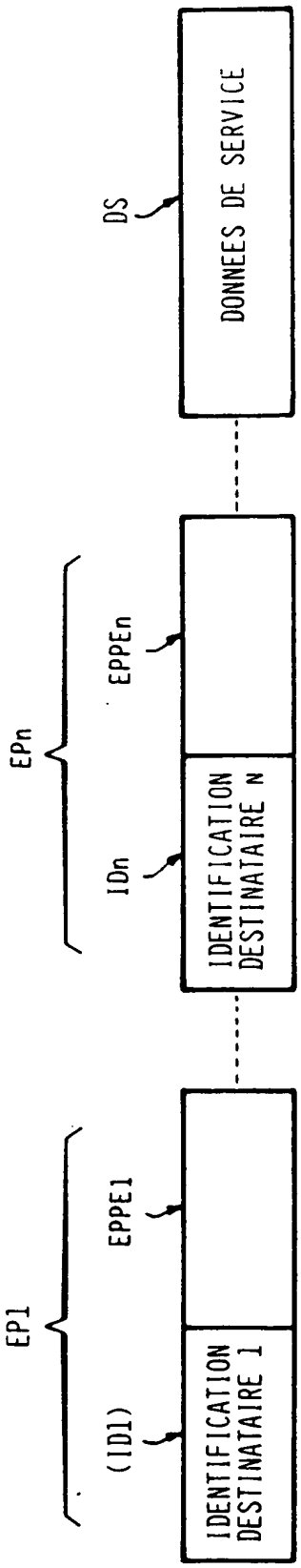
EP1
(ID1)
EPPE1
IDENTIFICATION DESTINATAIRE 1
EPn
IDn
EPPEn
IDENTIFICATION DESTINATAIRE N
DS
DONNEES DE SERVICE

FIG. 2

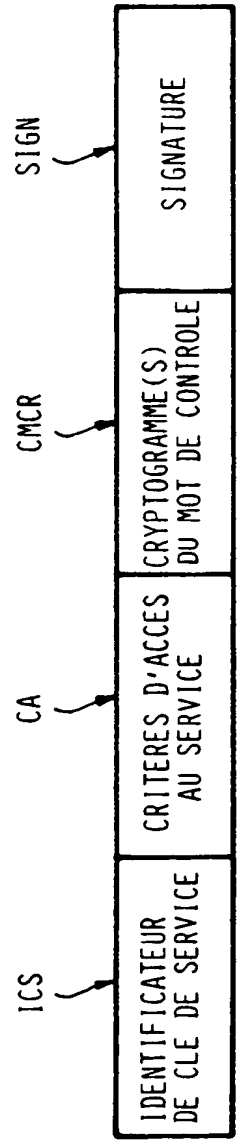
ICS
IDENTIFICATEUR DE CLE DE SERVICE
CA
CRITERES D'ACCES AU SERVICE
CMCR
CRYPTOGRAMME(S) DU MOT DE CONTROLE
SIGN
SIGNATURE

FIG. 3

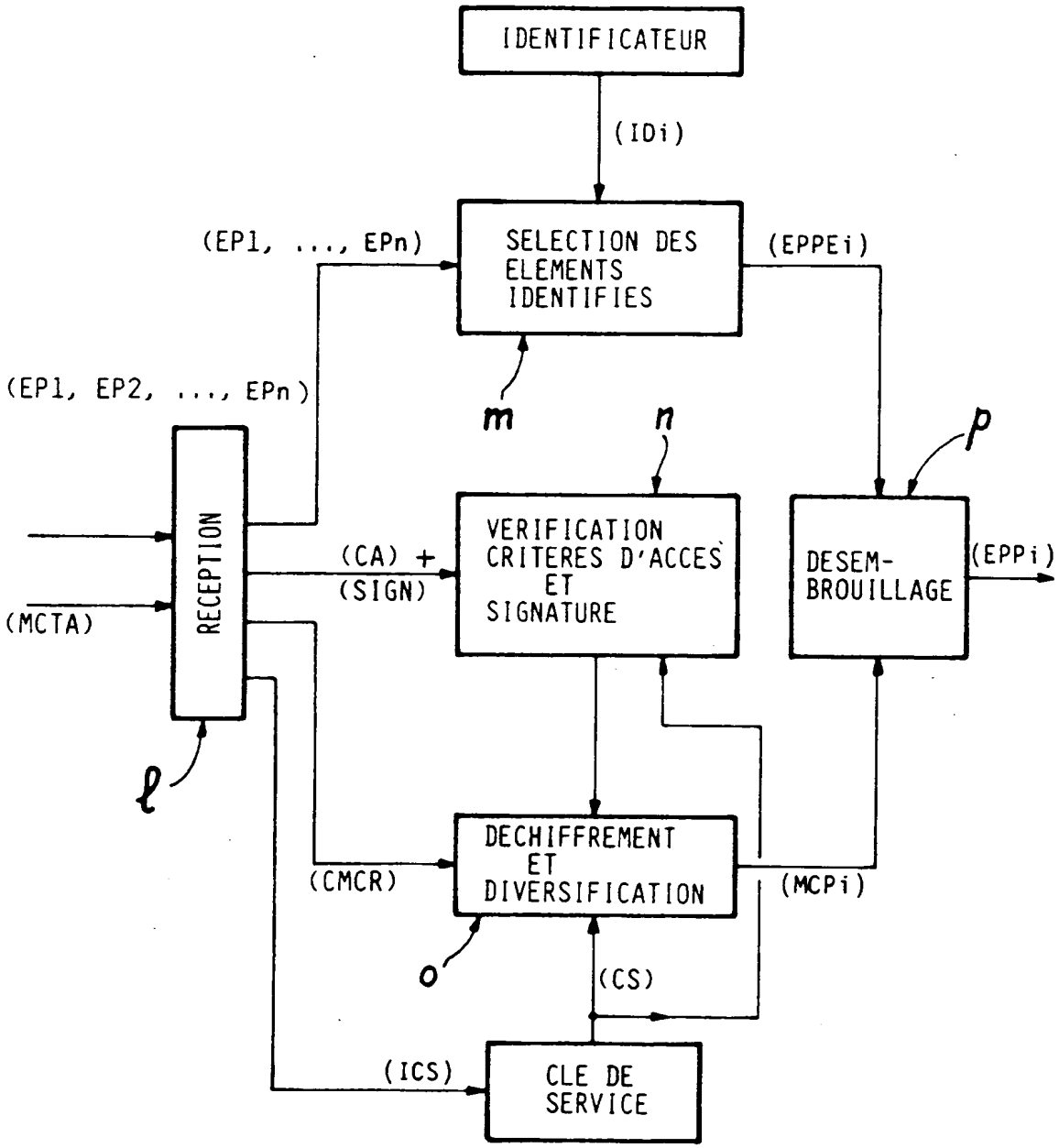
IDENTIFICATEUR
(IDi)
(EP1, ..., EPn)
SELECTION DES ELEMENTS IDENTIFIES
(EPPEi)
(EP1, EP2, ..., EPn)
m
n
p
RECEPTION
VERIFICATION CRITERES D'ACCES ET SIGNATURE
DESEM-BROUILLAGE
(EPPi)
(CA) + (SIGN)
(MCTA)
l
DECHIFFREMENT ET DIVERSIFICATION
(CMCR)
(MCPi)
o
(CS)
(ICS)
CLE DE SERVICE

FIG. 4

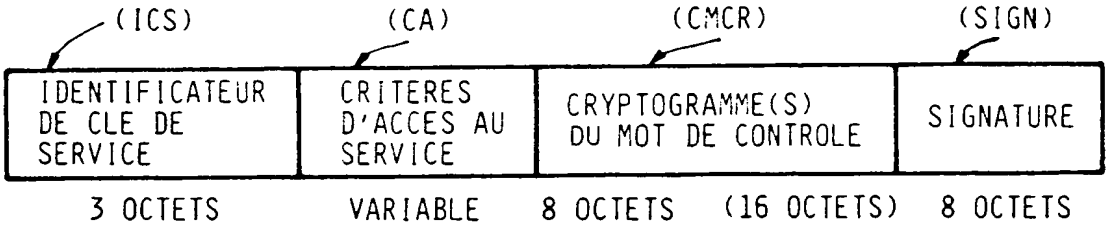

FIG. 5

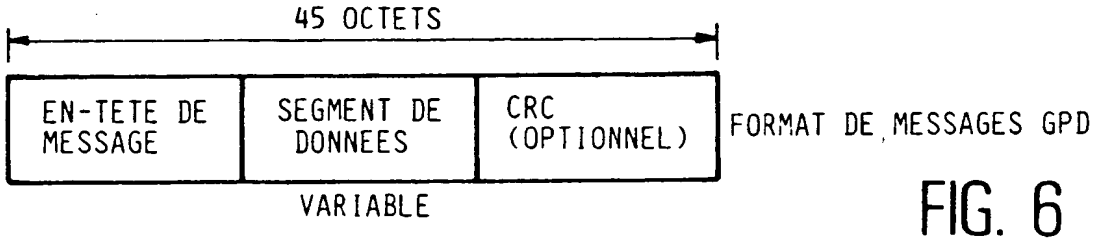

FIG. 6

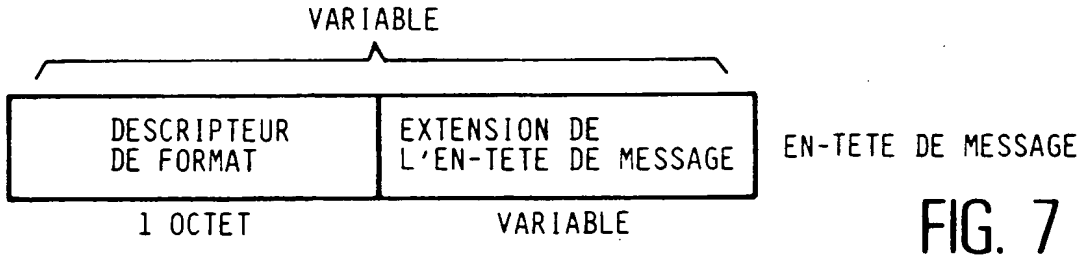

FIG. 7

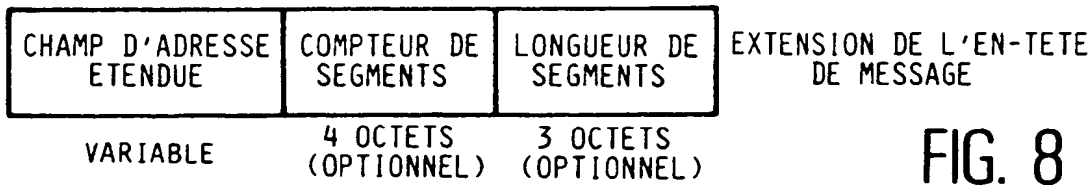

FIG. 8

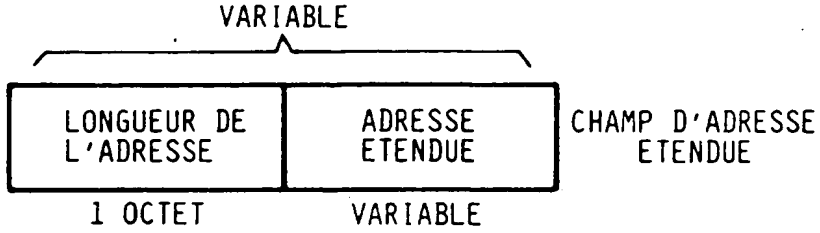

FIG. 9

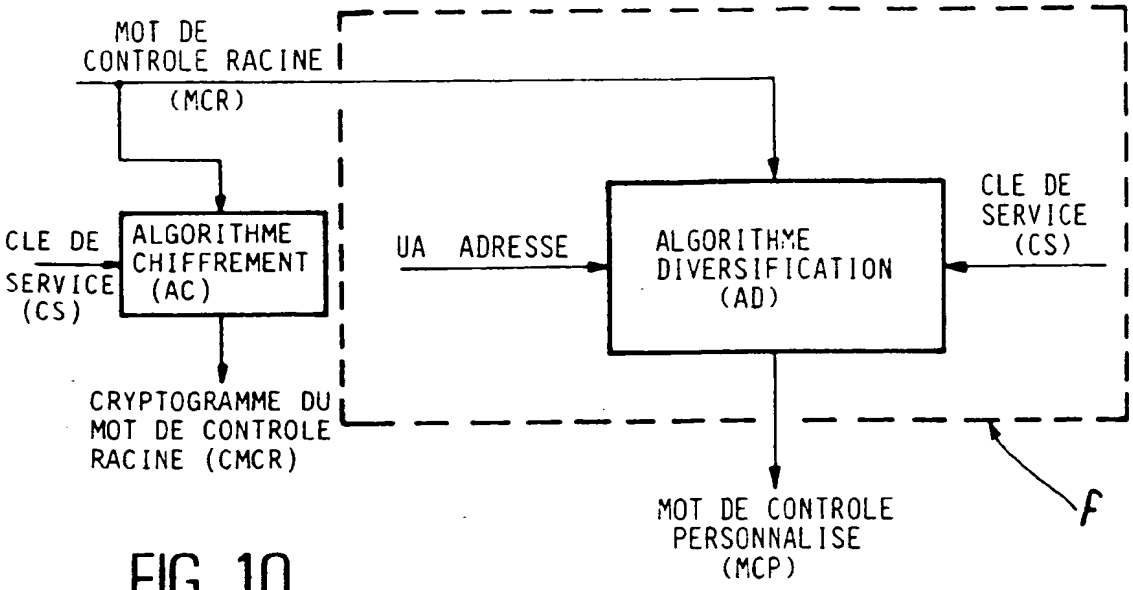
MOT DE
CONTROLE RACINE
(MCR)
CLE DE
SERVICE
(CS)
ALGORITHME
CHIFFREMENT
(AC)
CRYPTOGRAMME DU
MOT DE CONTROLE
RACINE (CMCR)
UA ADRESSE
ALGORITHME
DIVERSIFICATION
(AD)
CLE DE
SERVICE
(CS)
MOT DE CONTROLE
PERSONNALISE
(MCP)
f

FIG. 10

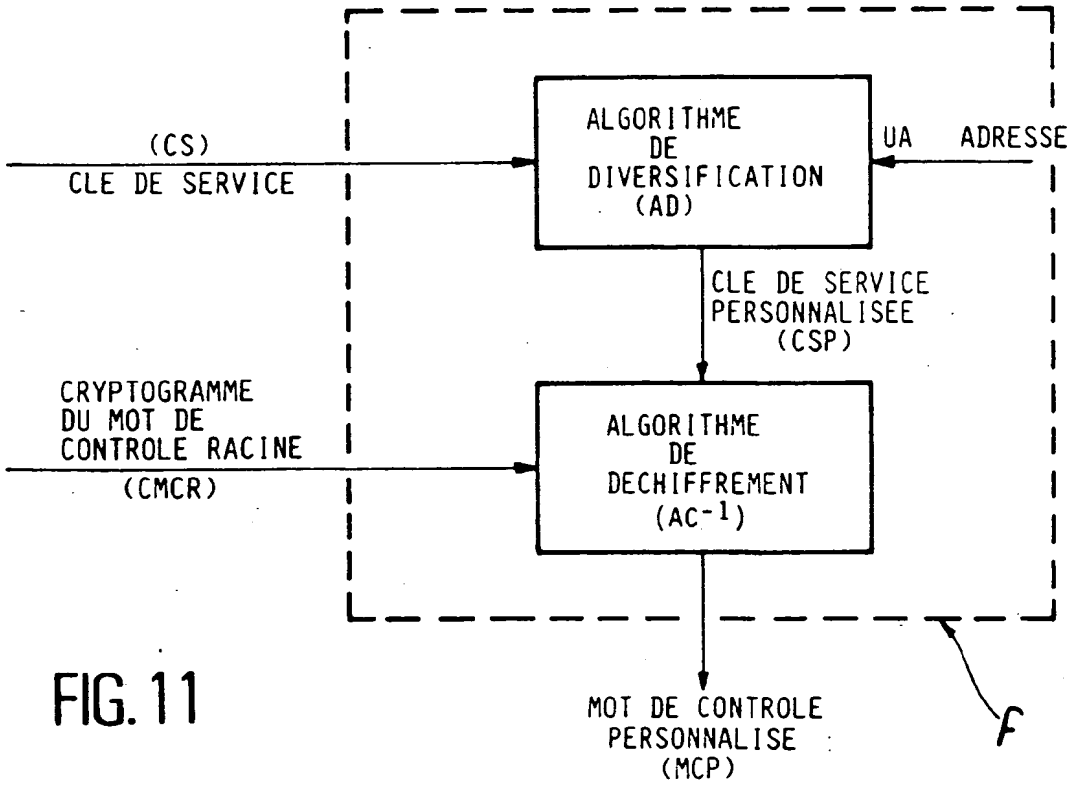
(CS)
CLE DE SERVICE
ALGORITHME
DE
DIVERSIFICATION
(AD)
UA ADRESSE
CLE DE SERVICE
PERSONNALISEE
(CSP)
CRYPTOGRAMME
DU MOT DE
CONTROLE RACINE
(CMCR)
ALGORITHME
DE
DECHIFFREMENT
(AC-1)
MOT DE CONTROLE
PERSONNALISE
(MCP)
f

FIG. 11

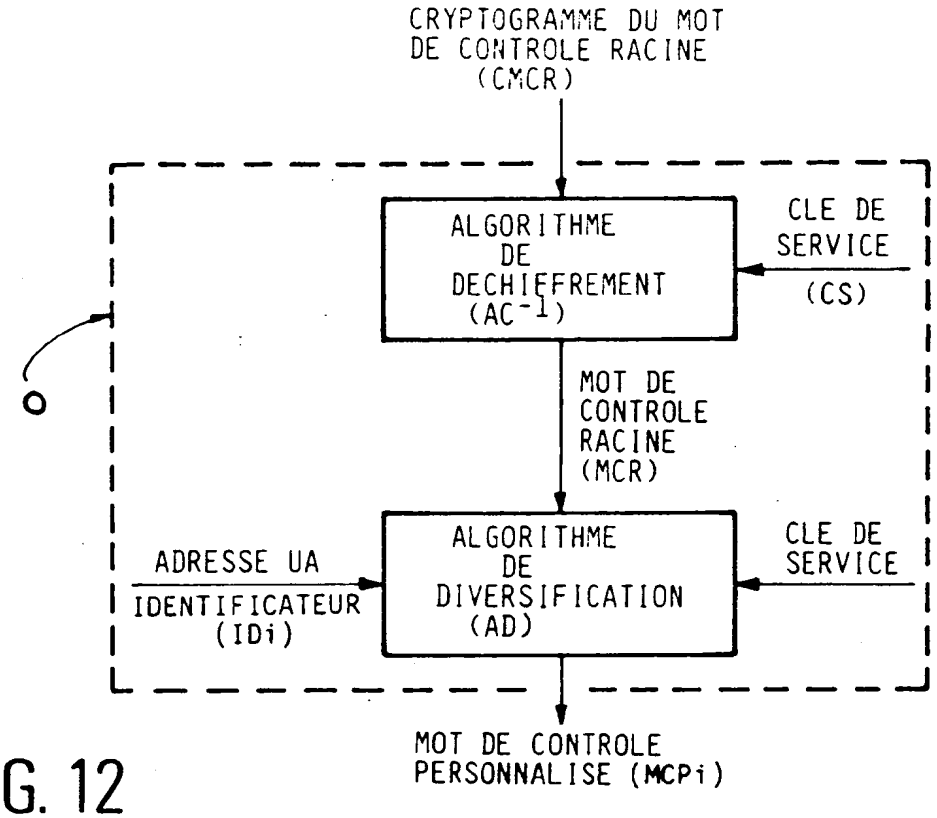
CRYPTOGRAMME DU MOT DE CONTROLE RACINE (CMCR)
ALGORITHME DE DECHIFFREMENT (AC^{-1})
CLE DE SERVICE (CS)
MOT DE CONTROLE RACINE (MCR)
ADRESSE UA
IDENTIFICATEUR (IDi)
ALGORITHME DE DIVERSIFICATION (AD)
CLE DE SERVICE
MOT DE CONTROLE PERSONNALISE (MCPi)

FIG. 12

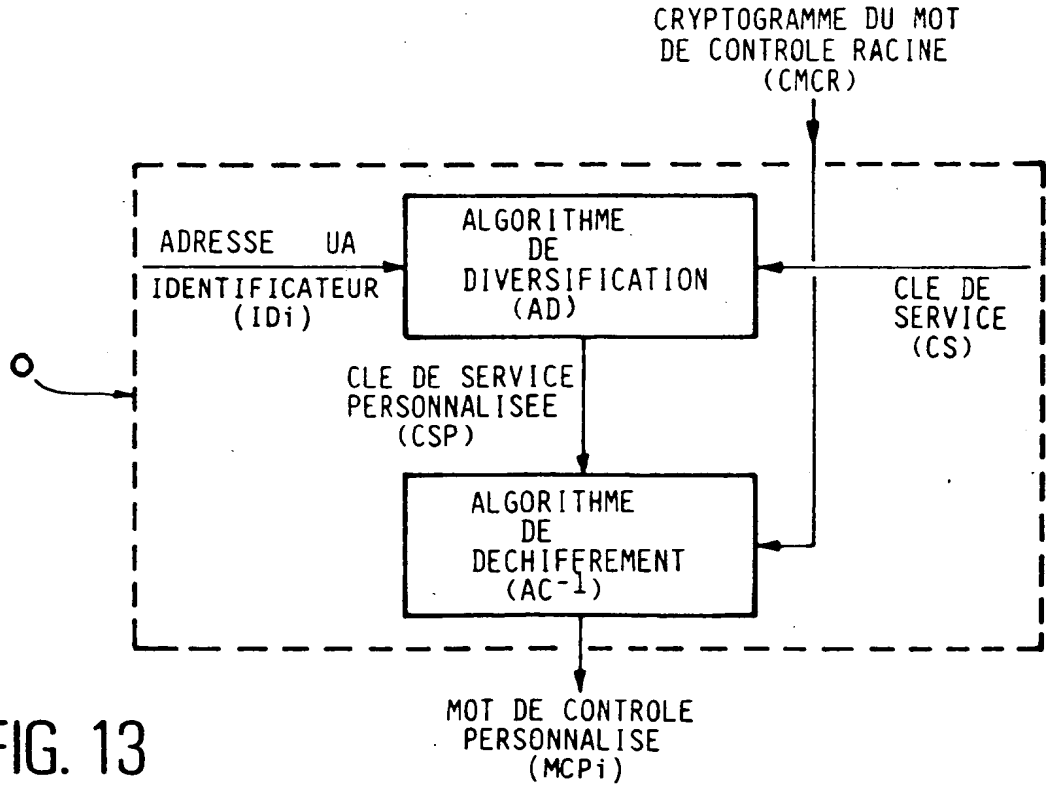
CRYPTOGRAMME DU MOT DE CONTROLE RACINE (CMCR)
ADRESSE UA
IDENTIFICATEUR (IDi)
ALGORITHME DE DIVERSIFICATION (AD)
CLE DE SERVICE (CS)
CLE DE SERVICE PERSONNALISEE (CSP)
ALGORITHME DE DECHIFFREMENT (AC^{-1})
MOT DE CONTROLE PERSONNALISE (MCPi)

FIG. 13

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 92 40 2294

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.5)
Y	EP-A-0 285 520 (BULL CP8) * abrégé; revendications *	1	G06F12/14
A		2-8	

Y	EP-A-0 277 247 (K.K. ADVANCE) * abrégé; revendications 1,2,9,10 *	1	
A		2-8	

Y	COMPUTERS & SECURITY. vol. 9, no. 6, Octobre 1990, AMSTERDAM NL pages 539 - 546 L.HARN ET AL. 'A cryptographic key generation scheme for multilevel data security' * page 539 - page 540 * * page 542, colonne de gauche, alinéa 3 *	1	
A		2-8	

A	PROC. COMP EURO 89 'VLSI AND COMPUTER PERIPHERALS', HAMBURG, MAY 8-12, 1989 TOPIC 4 pages 159 - 163 M.STEINACKER 'VLSI crypto-technology (application requirements)' * page 4-160, colonne de droite, alinéa 2 * * page 4-161, colonne de droite *	1-8	DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5) G06F H04L G07F

A	EP-A-0 427 601 (LABORATOIRE EUROPEEN DE RECHERCHES ELECTRONIQUES AVANCEES) * le document en entier *	1-8	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	07 OCTOBRE 1992	PFITZINGER E.E.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0402)